IMPACTOS DA TRANSIÇÃO E UTILIZAÇÃO DO IPV6 SOBRE A SEGURANÇA DE AMBIENTES COMPUTACIONAIS

Jansen Carlo Sena
Inst.Computação/Unicamp
13083-970 Campinas - SP
jansen.sena@ic.unicamp.br

Paulo Lício de Geus
Inst.Computação/Unicamp
13083-970 Campinas - SP
paulo@ic.unicamp.br

Alessandro Augusto
Inst.Computação/Unicamp
13083-970 Campinas - SP
alaugusto@yahoo.com.br

RESUMO

Do ponto de vista da segurança de sistemas, o IPv6 soluciona diversas fragilidades relativas ao IPv4, porém traz consigo a possibilidade do desenvolvimento de novos ataques. Desta forma, a identificação das suas potencialidades e problemas é fundamental para a auxiliar o processo de transição. Este artigo apresenta uma análise de segurança do IPv6, caracterizando suas soluções para ataques clássicos voltados ao IPv4, bem como novos problemas intrínsecos àquele protocolo.

1 Introdução

Quando o IPv4 foi projetado não se imaginavam as dimensões que a Internet iria alcançar. Inicialmente, sua tecnologia era voltada para o desenvolvimento de uma rede de computadores fundamentalmente acadêmica, com poucos requisitos.

O aumento exponencial do uso da Internet, que passou a ser utilizada pelos meios industriais, comerciais e domésticos, tornou inevitável o desenvolvimento de estruturas e mecanismos voltados ao IP capazes de prover suporte à novas necessidades. Um dos principais problemas identificados é a iminente exaustão do espaço de endereçamento do IPv4. Para solucionar tais problemas, o IETF (*Internet Task Engineering Force*) resolveu especificar uma nova versão para o protocolo IP, o IPv6. Porém, o projeto do IPv6 vai além de uma "versão do IPv4 com 128 bits de endereçamento".

Contudo, é suficiente pensar que junto com as soluções para fragilidades do IPv4, a especificação de um novo protocolo traz consigo um conjunto, ainda não bem definido, de problemas de segurança que devem ser, na medida do possível, identificados com o intuito de minimizar o impacto sobre a segurança dos sistemas em fase de transição para o IPv6.

Neste artigo, inicialmente, são apresentadas formas de evitar ataques clássicos ao IPv4 através do uso do IPv6. Em seguida, são identificadas fragilidades e possíveis ataques ao IPv6, bem como dificuldades que os seus mecanismos de segurança do IPv6 não são suficientes para proteger.

2 Estrutura geral do IPv6

Conhecidas as necessidades para o estabelecimento da nova versão do protocolo IP, apos muitas discussões, o IPv6 foi especificado, tendo como principais características o aumento do espaço de endereçamento para 128 *bits*, a simplificaçãoda sua estrutura e a incorporação de mecanismos de segurança e qualidade de serviço [4, 6].

Informações adicionais podem ser incluídas em pacotes IPv6 através do uso de cabeçalhos de extensão, inseridos, em uma ordem pré-determinada, entre o cabeçalho e a

porção de dados. Cada cabeçalho de extensão provê um serviço expecífico. Atualmente, a especificação do IPv6 contém a definição de seis cabeçalhos de extensão: *Hop-by-Hop Options*, *Routing*, *Fragment*, *AH*, *ESP* e *Destination Options* [4].

2.1 IPSec

O IPSec (*IP Security*) [1] é uma suíte de protocolos definida pelo IETF, cujo objetivo é possibilitar a utilização de serviços de autenticação, integridade e confidencialidade em pacotes. Tais serviços são providos através de dois cabeçalhos: o AH (*Authentication Header*)[2], utilizado para autenticar a origem dos dados e garantir a integridade dos mesmos até o destino; e o ESP (*Encapsulating Security Payload*)[3], utilizado para prover confidencialidade dos dados e, opcionalmente, autenticação e integridade. A implementação do IPSec no IPv6 é obrigatória, diferentemente do IPv4.

Diversos algoritmos criptográficos podem ser utilizados pelo AH e ESP. Porém, existe um conjunto mínimo cuja implementação é mandatória[1, 2, 3]. São eles: *HMAC-MD5-96* e *HMAC-SHA-1-96* para os serviços de autenticação e integridade do AH e ESP; DES-CBC para a confidencialidade provida pelo ESP; e, algoritmos nulos de autenticação e confidencialidade utilizados pelo ESP quando um dos seu serviços não é requisitado.

Para que duas entidades consigam enviar e receber pacotes utilizando os serviços do IPSec é necessário estabelecer uma associação de segurança (AS) que especifica os algoritmos a serem utilizados, as chaves criptográficas, os tempos de vida destas chaves, entre outros parâmetros. ASs são direcionais e só podem especificar um protocolo de segurança.

Existem duas maneiras para o estabelecimento de associações de segurança: estática e dinâmica. No primeiro, os parâmetros são inseridos manualmente em ambos os extremos da comunicação. No segundo, os parâmetros são negociados por protocolos como o IKE (*Internet Key Exchange*), sem qualquer intervenção do administardor.

3 Problemas de segurança no IPv4

O IPv4 não foi projetado para ser um protocolo com características de segurança. Inicialmente, seu uso estava restrito a um ambiente colaborativo onde existia uma "cooperação harmoniosa" entre os usuários. Porém, a popularização deste protocolo, dado seu uso na Internet, trouxe consigo a descoberta de um conjunto de falhas de segurança que podem ser exploradas por ataques que resultam desde DoS (*Denial of Service*) até invasões capazes de comprometer um sistema inteiro.

3.1 IP Spoofing

O *IP Spoofing*, uma das mais antigas e perigosas falhas encontradas no IPv4, consiste em enviar pacotes cujo endereço de origem não corresponde ao endereço da máquina que, de fato, os está enviando. Uma conseqüência natural do *IP Spoofing* é que possíveis pacotes de retorno serão enviados para a entidade falsificada e não para o falsificador.

Ataques como *smurf*, *hijacking* de conexão e o DNS *spoofing* [9] são possíveis graças a impossibilidade do IP detectar o *spoofing* de endereços. É importante notar que o *checksum*, presente em pacotes IPv4, é utilizado somente para detectar problemas durante a transmissão e pode ser calculado pelo próprio atacante após criar o pacote falsificado.

Caso o atacante necessite ter acesso aos pacotes de retorno e não esteja posicionado em um trecho das rotas, é possível utilizar a opção de *source routing* para forçar que os pacotes sigam um caminho que permita a sua captura. Se os roteadores não honrarem o processamento do *source routing*, o atacante pode basear-se no comportamento da aplicação utilizada. Por exemplo, como os procedimentos de abertura de uma conexão *telnet* são conhecidos, o atacante pode enviar respostas a pacotes que ele não capturou mas tem certeza que o *host* cujo endereço está sendo falsificado deveria tê-los enviado para a vítima.

3.2 Análise de tráfego

A análise de tráfego consiste em capturar pacotes no intuito de observar suas características e, principalmente, seu conteúdo. Inicialmente desenvolvida para atender as necessidades de administradores de sistemas, é um ataque passivo no qual o atacante precisa estar situado entre as duas entidades que estão se comunicando e, dadas suas características, torna-se difícil de ser detectada.

Aplicações, como POP3 e FTP, que não utilizam nenhum tipo de cifragem, permitem que o conteúdo transmitido, incluindo *logins* e senhas, seja obtido por um atacante que capture os pacotes correspondentes. Outras aplicações, que utilizam cifragem dos seus dados, como o SSH[9], ou mesmo mecanismos de proteção para o TCP, como o SSL (*Secure Socket Layer*) e o TLS (*Transport Socket Layer*), podem minimizar o impacto da análise de tráfego. Porém, isto não é completamente seguro (Seção 4.2).

3.3 Injeção e modificação de dados

Este é um tipo de ataque intermediário entre o *hijacking* e a análise de tráfego de uma conexão onde o atacante pode inteceptar um pacote, modificar seu conteúdo e repassá-lo ao destino. A única precaução que o atacante deve ter é recalcular o *checksum*. Outra maneira de realizar este ataque é através da injeção de pacotes falsos, na tentativa de que eles cheguem antes dos pacotes originais, invalidando os mesmos perante seu destino e fazendo com que este processe pacotes com conteúdo malicioso.

3.4 Replay

O ataque de *replay* consiste em salvar os pacotes transmitidos por uma comunicação entre duas entidades e depois reutilizá-los na tentativa de forjar uma nova comunicação.

Em alguns casos, mesmo o conteúdo cifrado pode ser alvo deste ataque. Em outras palavras, o atacante pode não conhecer o conteúdo exato de alguns pacotes, mas pode ter ciência de que se trata da abertura de uma sessão, por exemplo, e, portanto, eles devem conter dados como *login* e senha. Desta forma, se não existirem mecanismos para evitar a reutilização destes dados, este tipo de ataque torna-se muito factível. *Replay* também pode ser realizado, caso seja possível extrair porções corretas de texto cifrado associadas a informações importantes. Por exemplo, mesmo não conhecendo uma senha, para este tipo de ataque, obter o texto cifrado correspondente representa um passo importante.

Replay de dados baseados em aplicações que utilizam TCP não é tão simples, dado que este protocolo utiliza números de seqüência para controle. Por outro lado, este ataque pode funcionar facilmente em protocolos baseados em UDP.

4 Soluções de segurança no IPv6

O IPv6 foi projetado com o objetivo de solucionar os problemas e deficiências detectados no IPv4. Em relação à segurança, a principal característica do IPv6 foi a incorporação do IPSec na sua especificação. Apesar do IPSec também poder ser utilizado com o IPv4, ele não é nativo neste protocolo e, portanto, sua utilização transparente torna-se inviável, dado o alto custo das modificações em muitas implementações.

Os serviços providos pelo IPSec, através dos cabeçalhos AH e ESP, podem ser utilizados para resolver parte dos problemas de segurança do IPv4 relacionados na Seção 3.

4.1 IP Spoofing

O AH não seria seguro se os seus serviços, autenticação e integridade, não fossem oferecidos em conjunto.

A autenticação garante que um determinado pacote realmente tenha sido enviado pela entidade identificada como emissora. Porém, não há nenhuma garantia se ele foi ou não modificado durante seu percuso até o destino. Tal proteção advém da integridade dos dados. A combinação destes dois serviços é capaz de garantir se um pacote realmente pertence a uma determinada origem e se o seu conteúdo foi alterado.

Em virtude do *IP Spoofing* basear-se na falsificação do endereço de origem, o uso do AH obriga o atacante a calcular um *hash* semelhante àquele que seria gerado pela entidade que está sendo falsificada, sendo necessário para tal a obtenção dos parâmetros de uma possível AS estabelecida entre a vítima e esta entidade, incluindo as chaves criptográficas e os algoritmos. Caso contrário, ao receber o pacote forjado e verificar a diferença entre o *hash* recebido e o calculado, a vítima descarta-lo-á.

4.2 Análise de tráfego

Para evitar que um atacante, situado no caminho entre duas entidades, consiga capturar pacotes para analisar seu conteúdo, incluindo dados dos protocolos IP, TCP e de aplicação, pode-se utilizar o cabeçalho ESP para a cifragem dos dados, provendo confidencialidade transparente aos dados de toda e qualquer aplicação.

O ESP no modo de transporte, porém, não previne a análise dos dados contidos no cabeçalho IP e nos cabeçalhos de extensão anteriores ao ESP. Por outro lado, no modo de tunelamento, o pacote original completo fica protegido em relação à análise do seu conteúdo.

Vale ressaltar que a análise de tráfego pode basear-se em outros parâmetros além do conteúdo dos pacotes. Criptoanalistas podem considerar informações de pacotes como: a origem e o destino, a quantidade em um determinado período de tempo, o tamanho e a freqüência. Tais informações não podem ser protegidas com o ESP. Uma maneira de tentar evitar a obtenção destas informações é a utilização de cifragem na camada de enlace de dados.

4.3 Injeção e modificação de dados

A utilização de cifragem de dados, nos níveis de aplicação, protocolo de transporte ou protocolo de rede, não são capazes de prevenir este ataque. Apesar do atacante, neste

caso, não conseguir ter acesso a informações legíveis, os dados falsos inseridos podem atrapalhar ou, até mesmo, inviabilizar a conexão[9].

A forma de garantir proteção contra a injeção e/ou modificação de dados através do IPSec é com o uso do AH. Neste caso, qualquer modificação nos dados de um pacote irá acarretar na incompatibilidade do *hash* presente no AH. Conseqüentemente, para injetar pacotes válidos, da mesma forma que no IP *spoofing*, o atacante necessita gerar um *hash* correspondente, baseado no algoritmo e na chave criptográfica utilizados pela verdadeira origem dos dados.

É importante observar que a injeção/modificação pode ocorrer nos dados de qualquer protocolo. Sendo assim, como a autenticação especificada no ESP garante a origem e a integridade somente dos dados cifrados, este protocolo não é capaz de oferecer proteção contra este tipo de ataque.

4.4 Replay

Tanto o AH como o ESP possuem mecanismos para prover proteção contra *replay* de pacotes[1]. Em ambos os cabeçalhos existe um campo que armazena um número de seqüência, cujo valor inicial é aleatório, para que o receptor consiga identificar pacotes antigos. Porém, sob certas circunstâncias, ataques de *replay* podem obter sucesso mesmo na presença do IPSec (Seção 5.2).

5 Fragilidades do IPv6

Apesar do projeto do IPv6 ter sido norteado pela necessidade de correção das fragilidades do IPv4, é razoável pensar que novas fragilidades deverão ser evidenciadas.

5.1 IPv6 sem autenticação, integridade e cifragem

Apesar do IPSec estar presente como parte integrante do IPv6, o seu uso não é obrigatório. Desta forma, utilizar o IPv6 sem os serviços do IPSec, torna-o vunerável a diversos ataques já conhecidos do IPv4 e a ataques que podem ser desenvolvidos a partir dos novos mecanismos utilizados pelo IPv6.

Por exemplo, o *Router Discovery*, definido como parte do ICMPv6 possibilita que roteadores sinalizem sua presença para os *hosts* presentes no mesmo trecho de rede através da mensagem *ICMP Router Advertisement*[6]. Tais mensagens podem conter parâmetros como o *Hop Limit* máximo a ser utilizado pelos *hosts* e o tempo em que cada *host* deve utilizar o roteador como *default*. Este processo é suscetível a um conjunto de ataques quando não utiliza a autenticação do pacote IP.

Considere a situação onde um atacante, *Attacker*, envia uma mensagem para *Victim* falsificando *Router*, fazendo com que *Victim* utilize "1" para o campo *Hop Limit* dos seus pacotes a serem enviados. A mensagem ICMP falsa ainda instrui *Victim* a guardar tais configurações pelo maior tempo possível (65.536ms). Sendo assim, todo pacote enviado por *Victim* destinado à Internet não será entregue, dado que *Router* não irá repassar pacotes com *Hop Limit* expirado. Como conseqüência, *Victim* irá receber uma mensagem

[1]No ESP o serviço de proteção contra *replay* é opcional, provido em conjunto com o serviço de autenticação/integridade dos dados cifrados.

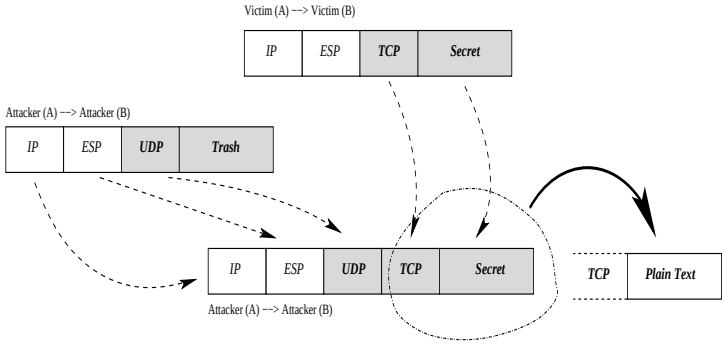

Figura 1: Exemplo de *cut-and-paste*.

ICMP. Este procedimento constitui um ataque de DoS e pode ser utilizado para atingir todas as máquinas da rede.

Outra forma de explorar o *Router Discovery* sem a presença do IPSec (AH) seria através da divulgação de um falso roteador a todos os *hosts*, fazendo com que estes enviem pacotes que certamente serão perdidos.

É possível, ainda, submeter o IPv6, sem o uso do IPSec, a diversos ataques identificados no IPv4. Por exemplo, da mesma forma que no IPv4 pode-se injetar no campo *Options* o *source routing*, no IPv6, pode-se injetar um cabeçalho *Routing* contendo esta opção.

5.2 IPv6 somente com cifragem

O IPSec pode ser utilizado de diversas maneiras, com o AH ou ESP, ou ambos. Além disso, as AS podem ter granularidade distintas. Por exemplo, da mesma forma que uma única AS pode ser utilizada para proteger todos os dados entre dois *hosts*, uma AS pode ser requisitada para cada conexão ou ainda para cada usuário. Um caso especial do uso do IPSec é quando se utilizam somente ESP e ASs baseadas em *host*. Neste caso, as chaves criptográficas dos *hosts* são fixas para toda a comunicação entre eles. A seguir serão apresentados ataques baseados neste cenário.

5.2.1 Ataques de cut-and-paste

Considere que um usuário, *Victim*, está abrindo uma conexão *telnet* de um *host* A para um *host* B, de acordo com o cenário descrito anteriormente. Outro usuário, *Attacker*, captura os pacotes iniciais e envia um pacote UDP de A para B, contendo dados quaisquer na porção de dados, e armazena o seu conteúdo. Em seguida, *Attacker* insere na porção de dados do pacote UDP os dados cifrados, contendo o cabeçalho TCP e os dados da aplicação de um pacote capturado de *Victim*, e então reenvia este pacote de A para B. Como estes dois *hosts* utilizam a mesma chave para toda comunicação entre eles, elas serão utilizadas para o tráfego de ambos os usuários. Propriedades dos algoritmos de cifragem baseados em blocos, utilizados pelo ESP, farão com que a decifragem do pacote UDP recupere informações contidas na porção de dados, incluindo uma porção do cabeçalho TCP (dependendo do tamanho do bloco) e, provavelmente, toda a porção de dados do pacote de *Victim*, conforme mostrado na Figura 1. Tal técnica denomina-se *cut-and-paste*.

Se este procedimento for repetido em todos os pacotes iniciais capturados, entre os dados decifrados, certamente estarão o *login* e senha da vítima. Este mesmo cenário

torna-se mais fácil IPv4, uma vez que, neste protocolo, o *checksum* gerado pelo UDP pode ser desabilitado. Por outro lado, mesmo que o UDP no IPv6 gere um *checksum*, somente 2^{16} tentativas serão necessárias para reinjetar o pacote com sucesso.

5.2.2 Hijacking

Utilizar somente a cifragem de dados não é suficiente para evitar *hijacking* de conexão. Considere que um atacante captura um pacote legítimo da vítima originado de um *host* A para um *host* B. Em seguida, o atacante envia um pacote UDP de A para B contendo, na porção de dados informações a serem inseridas na conexão da vítima.

Caso o pacote original da vítima consiga ser deletado, o atacante pode simplesmente substituir o seu *payload* e enviar este pacote. Caso negativo, será necessário construir um novo pacote contendo o cabeçalho TCP cifrado do pacote da vítima e *payload* contendo instruções maliciosas geradas no pacote enviado pelo atacante. Em ambos os casos será necessário inserir blocos de dados de acordo com o tamanho do bloco utilizado pelo algoritmo de cifragem.

5.3 Cabeçalhos de extensão

Os cabeçalhos de extensão possuem uma ordem específica de encadeamento, porém as implementações devem estar preparadas para processá-los em qualquer ordenação[4].

Ataques voltados para erros de implementação podem ser desenvolvidos através do envio de pacotes com cabeçalhos em ordens diversas contendo cabeçalhos duplicados, entre outros, na tentativa de descobrir problemas na pilha IPv6, como *buffer overflow* ou *crashes*.

Em relação à especificação, fragilidades poderão ser exploradas quando novas opções foram definidas para os cabeçalhos *Hop-by-Hop Options* e *Destination Options*. Em tais cabeçalhos, existem opções cujos valores são alterados em trânsito e, portanto, não entram no *checksum* gerado pelo AH. Desta forma, pode ser possível capturar pacotes, alterar os valores de tais opções ou, até mesmo, substituir por outras opções, provocando efeitos ainda não conhecidos.

5.4 Algoritmos criptográficos e escalabilidade do IPSec

O IPSec suporta a utilização de diversos algoritmos criptográficos com o AH e ESP. Porém, o conjunto obrigatório não é suficiente para prover segurança adequada a todos os tipos de informação.

Estudos têm mostrado que particularidades do MD5 permitem acelerar o processo para gerar mensagens que produzam o mesmo *hash* utilizando máquinas de baixo custo [7]. Em relação ao DES, o tamanho da chave utilizada, 56 *bits*, é, atualmente, vulnerável a ataques de força-bruta tornando-o inadequado para preservar informações cujo sigilo é de extrema significância[7].

A implementação de outros algoritmos pode ser útil somente entre sistemas isolados. Se algoritmos mais seguros não estão padronizados, nem todas as implementações os conterão. Além disso, o IPSec não possui diferenciação entre quais algoritmos utilizar para a comunicação de diferentes serviços.

A escalabilidade do IPSec está relacionada ao estabelecimento dinâmico de ASs que devem ser definidas por conexão ou, no máximo, por usuário, para prover maior segurança.

Abusar, intencionalmente, do mecanismo de estabelecimento de ASs, pode constituir diversos ataques de DoS. Como o IPSec é fundamental para a segurança do IPv6, é de extrema importância encontrar soluções para prevenir tais possibilidades.

6 Conclusões

O desenvolvimento do IPv6 visa adaptar este protocolo à novos requisitos da Internet contemporânea não contemplados na sua versão anterior. Porém, apesar de impedir um conjunto de vulnerabilidades exploradas no IPv4 ao longo dos anos, o IPv6 certamente não é uma panacéia para a camada de rede.

O uso de algoritmos criptográficos por parte do IPSec, nativo no IPv6, pode provocar uma "falsa sensação de segurança". O transporte seguro de pacotes não é capaz de imunizar fragilidades em aplicações nem tampouco proteger contra falhas decorrentes da administração de um sistema. Desta forma, os cenários identificados neste trabalho visam colaborar na mensuração dos impactos de segurança que o IPv6 trará consigo, em especial durante o período de transição.

Outros esforços neste sentido vêm sendo empenhados no intuito de viabilizar a utilização deste protocolo que, certamente, irá servir como um dos alicerces para a manutenção da Internet nas próximas décadas.

Referências

[1] Kent, S., Atkinson, R. (1998). *Security Architecture for the Internet Protocol*. RFC 2401. Internet Engineering Task Force.

[2] Kent, S., Atkinson, R. (1998). *IP Authentication Header*. RFC 2402. Internet Engineering Task Force.

[3] Kent, S., Atkinson, R. (1998). *IP Encapsulating Security Payload (ESP)*. RFC 2406. Internet Engineering Task Force.

[4] Deering, S., Hinden, R. (1998). *Internet Protocol, Version 6 (IPv6) Specification*. RFC 2460. Internet Engineering Task Force.

[5] Bellovin, S. (1996). *Problem Areas For The IP Security Protocols*. Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California.

[6] Huitema, C. (1997). *IPv6 The New Internet Protocol*. 2nd Edition. Prentice Hall.

[7] Schneier, B. (1996). *Applied Cryptography*. 2nd Edition. John Wiley & Sons.

[8] Stevens, R. W. (1994). *TCP/IP Illustrated, Volume I: The Protocols*. Addison-Wesley.

[9] Zwicky, E. D., Cooper, S., Chapman, D. B. (2000). *Building Internet Firewalls*. 2nd Edition, O'Reilly and Associates.